CLAIMS

What is claimed is:

1. A data structure to index an object captured during transmission from an origination address to a destination address, the data structure comprising:

a source address field to indicate an origination address of the object;

a destination address field to indicate a destination address of the object;

a source port field to indicate an origination port of the object;

a destination port field to indicate a destination port of the object;

a content field to indicate a content type from a plurality of content types identifying a type of content contained in the object; and

a time field to indicate when the object was captured.

2. The data structure of claim 1, wherein the plurality of content types comprises JPEG, GIF, BMP, TIFF, PNG, Skintone, PDF, MSWord, Excel, PowerPoint, MSOffice, HTML, WebMail, SMTP, Telnet, Rlogin, FTP, Chat, GZIP, ZIP, TAR, C++ Source, C Source, FORTRAN Source, Verilog Source, C Shell, K Shell, Bash Shell, Plaintext, Crypto, LIF, Binary Unknown, ASCII Unknown, and Unknown.

3. The data structure of claim 1, further comprising a device identity field to indicate a device that captured the object.

4. The data structure of claim 1, further comprising a protocol field to indicate the protocol that carried the object.

5. The data structure of claim 1, further comprising an instance field to indicate a number of the object in a connection.

6. The data structure of claim 1, further comprising an encoding field to indicate a how the object was encoded.

7. The data structure of claim 1, further comprising a size field to indicate the size of the object.

8. The data structure of claim 1, further comprising an owner field to indicate an entity that requested capture of the object.

9. The data structure of claim 1, further comprising a capture rule field to indicate a rule that triggered capture of the object.

10. The data structure of claim 1, further comprising a signature field to store a signature of the object.

11. The data structure of claim 10, wherein the signature comprises a digital cryptographic signature.

12. The data structure of claim 1, further comprising a tag signature field to store a signature of the data structure.

13. The data structure of claim 12, wherein the tag signature comprises a digital cryptographic signature.

14. A tag storing relational data over an object captured by a capture system, the relational data comprising:

an Ethernet controller MAC address of the capture system that captured the object;

a source Ethernet IP address of the object;

a destination Ethernet IP address of the object;

a source TCP/IP port number of the object;

a destination TCP/IP port number of the object;

an IP protocol that carried the object when captured by the capture system;

a canonical count of a number of the object within a TCP/IP connection;

a content type of the object;

an encoding that was used on the object;

the size of the object;

a timestamp indicating when the capture system captured the object;

a user who requested capture of the object;

a capture rule that directed capture of the object;

a hash signature of the object; and

a hash signature of the tag.

15. The tag of claim 14, wherein the hash signature of the object comprises a digital cryptographic signature of the object.

16. The tag of claim 15, wherein the hash signature of the tag comprises a digital cryptographic signature of the tag.

17. The tag of claim 14, wherein the content type of the object is one of JPEG, GIF, BMP, TIFF, PNG, Skintone, PDF, MSWord, Excel, PowerPoint, MSOffice, HTML, WebMail, SMTP, Telnet, Rlogin, FTP, Chat, GZIP, ZIP, TAR, C++ Source, C Source, FORTRAN Source, Verilog Source, C Shell, K Shell, Bash Shell, Plaintext, Crypto, LIF, Binary Unknown, ASCII Unknown, and Unknown.

18. A method comprising:

searching a plurality of tags, each tag indexing an object captured during transmission from an origination address to a destination address, the search using one or more of a plurality of tag fields, the tag fields comprising a source address field to indicate an origination address of the object, a destination address field indicating a destination address of the object, a source port field indicting an origination port of the object, a destination port field indicating a destination port

of the object, a content field indicating a content type from a plurality of content types identifying a type of content contained in the object, and a time field indicating when the object was captured.

19. The method of claim 18, wherein the plurality of tag fields further comprises a size field to indicate the size of the object.

20. The method of claim 18, further comprising displaying tags found as a result of the search.

21. A method comprising:

searching a tag database using one or more search criteria, the search resulting in at least one tag;

verifying the tag using a cryptographic tag signature;

retrieving an object indexed by the tag;

verifying the object using a cryptographic signature of the object; and

22. The method of claim 21, further comprising presenting the verified object to a user.

23. The method of claim 21, wherein the cryptographic tag signature and the cryptographic signature of the object are stored in the tag.

24. The method of claim 21, wherein verifying the object comprises calculating a hash of the object, decrypting the cryptographic signature of the object with a public key, and comparing the hash of the object with the decrypted signature.

25. The method of claim 21, further comprising generating a warning to the user if at least one of the object and the tag could not be verified.